Resumen 6 y 7

Daniel Barrantes Esquivel

Redes

ALGORITMOS DE CLAVE SIMÉTRICA

Los algoritmos de clave simétrica: se utilizan la misma clave para encriptar y desencriptar. Los cifrados en bloques: toman un bloque de n bits de texto llano como entrada y lo transforman utilizando la clave en un bloque de n bits de texto cifrado Los algoritmos criptográficos pueden implementarse ya sea en hardware (para velocidad) o en software (para flexibilidad). Aunque la mayoría tiene que ver con algoritmos y protocolos, que son independientes de la implementación real, no están de más unas cuantas palabras acerca de la construcción de hardware criptográfico. Las transposiciones y las sustituciones pueden implementarse mediante circuitos eléctricos sencillos.

Los cifrados de producto que operan en entradas de k bits para generar salidas de k bits son muy comunes. Por lo general, k es 64 a 256. Una implementación de hardware por lo general tiene por lo menos 18 etapas físicas. Una implementación de software se programa como un ciclo con por lo menos 8 iteraciones, cada una de las cuales realiza sustituciones de tipo caja S en sub bloques del bloque de datos de 64 a 256 bits, seguido por una permutación que mezcla las salidas de las cajas S. Con frecuencia hay una permutación inicial especial y también una al final. En la literatura, las iteraciones se conocen como rondas.

DES—El Estándar de Encriptación de Datos

En cada una de las 16 iteraciones, se usa una clave diferente. Antes de iniciarse el algoritmo, se aplica una transposición de 56 bits a la clave. Justo antes de cada iteración, la clave se divide en dos unidades de 28 bits, cada una de las cuales se gira hacia la izquierda una cantidad de bits dependiente del número de iteración. Ki se deriva de esta clave girada aplicándole otra transposición de 56 bits. En cada vuelta se extrae y permuta de los 56 bits un subgrupo de 48 bits diferente.

En 1977, dos investigadores de criptografía de Stanford, Diffie y Hellman (1977) diseñaron una máquina para violar el DES y estimaron que el costo de la construcción podría ascender a unos 20 millones de dólares. Dado un trozo pequeño de texto llano y el texto cifrado correspondiente, esta máquina podría encontrar la clave mediante una búsqueda exhaustiva del espacio de claves de 2 elevado a 56 entradas en menos de un día. Hoy día tal máquina costaría tal vez menos de un millón de dólares.

Triple DES

Se utilizan dos claves y tres etapas. En la primera etapa, el texto llano se encripta mediante DES de la forma usual con K1. En la segunda etapa, DES se ejecuta en modo de desencriptación, utilizando K2 como la clave.

La razón para encriptar, desencriptar y luego encriptar de nuevo es la compatibilidad hacia atrás con los sistemas DES de una sola clave. Tanto las funciones de encriptación como de desencriptación son correspondencias entre grupos de números de 64 bits. Desde el punto de vista criptográfico, las dos correspondencias son igualmente robustas.

Sin embargo, mediante el uso de EDE en lugar de EEE, una computadora que emplea triple encriptación puede comunicarse con otra que usa encriptación sencilla simplemente estableciendo K1 = K2. Esta propiedad permite la introducción gradual de la triple encriptación, algo que no interesa a los criptógrafos académicos, pero que es de importancia considerable para IBM y sus clientes.

AES—El Estándar de Encriptación Avanzada

El NIST adoptó una estrategia sorprendentemente diferente para una burocracia gubernamental: promovió un concurso. En enero de 1997, los investigadores de todo el mundo fueron invitados a emitir propuestas para un nuevo estándar, que se llamaría AES (Estándar de Encriptación Avanzada)

En octubre de 2000, el NIST anunció que él también votó por Rijndael, y en noviembre de 2001 Rijndael se volvió un estándar del gobierno de Estados Unidos publicado como FIPS 197 (Estándar Federal para el Procesamiento de Información). Debido a la extraordinaria apertura de la competencia, las propiedades técnicas de Rijndael y al hecho de que el equipo ganador estuvo compuesto por dos jóvenes criptógrafos belgas (quienes no es probable que hayan construido una puerta trasera sólo para complacer a la NSA), se espera que Rijndael se vuelva el estándar criptográfico dominante en el mundo por lo menos por una década. El nombre Rijndael se deriva de los apellidos de los autores: Rijmen + Daemen.

Rijndael

Rijndael utiliza sustitución y permutaciones, así como múltiples rondas. El número de rondas depende del tamaño de clave y del tamaño de bloque, y es de 10 para las claves de 128 bits con bloques de 128 bits y aumenta hasta 14 para la clave o el bloque más grande. Sin embargo, a diferencia del DES, todas las operaciones involucran bytes completos, para permitir implementaciones eficientes tanto en hardware como en software.

El código inicia expandiendo la clave en 11 arreglos del mismo tamaño que el estado. Éstos se almacenan en rk, que es un arreglo de estructuras, cada una de las cuales contiene un arreglo de estado. Uno de los arreglos se utilizará al inicio del cálculo y los otros 10 se utilizarán en 10 rondas, uno por ronda. El cálculo de las claves de ronda de la clave de encriptación es muy complicado para tratarlo aquí. Basta decir que las claves de ronda se producen mediante una rotación repetida y aplicando OR exclusivo a varios grupos de bits de clave.

Modos de cifrado

A pesar de toda esta complejidad, el AES (o el DES o, de hecho, cualquier cifrado de bloques) es básicamente un cifrado de sustitución monoalfabética que utiliza caracteres grandes (caracteres de 128 bits para el AES y caracteres de 64 bits para el DES). Siempre que el mismo bloque de texto llano entra en la etapa inicial, el mismo bloque de texto cifrado sale de la etapa final. Si encripta 100 veces el texto llano abcdefgh con la misma clave DES, obtiene 100 veces el mismo texto cifrado. Un intruso puede aprovechar esta propiedad para violar el cifrado.

Modo de libro de código electrónico

Para ver cómo puede utilizarse esta propiedad de cifrado de sustitución monoalfabética para vencer parcialmente el cifrado, utilizaremos el (triple) DES porque es más fácil diseñar bloques de 64 bits que de 128 bits, pero el AES tiene exactamente el mismo problema. La forma directa de utilizar el DES para cifrar una pieza grande de texto llano es dividirla en bloques consecutivos de 8 bytes (64 bits) y encriptarlos

después uno tras otro con la misma clave. La última pieza de texto llano se rellena a 64 bits, en caso de ser necesario.

Esta técnica se conoce como modo ECB (modo de Libro de Código Electrónico) en analogía con los libros de código pasados de moda en los que se listaba cada palabra de texto llano, seguida por su texto cifrado (por lo general, un número decimal de cinco dígitos).

Un archivo de computadora que lista los bonos anuales que una compañía ha decidido otorgar a sus empleado, consiste en registros consecutivos de 32 bytes, uno por empleado, en el formato que se muestra: 16 bytes para el nombre, 8 bytes para el puesto y 8 bytes para el bono. Cada uno de los 16 bloques de 8 bytes (numerados del 0 al 15) se encripta mediante (triple) DES.

Modo de encadenamiento de bloques de cifrado

En este método, cada bloque de texto llano se le aplica un OR exclusivo con el bloque anterior de texto cifrado antes de ser encriptado. En consecuencia, el mismo bloque de texto llano ya no corresponde con el mismo bloque de texto cifrado, y la encriptación deja de ser un enorme cifrado de sustitución monoalfabética. Al primer bloque se le aplica un OR exclusivo con un IV (Vector de Inicialización) elegido de manera aleatoria, que se transmite (en texto llano) junto con el texto cifrado El encadenamiento de bloques cifrado también tiene la ventaja de que el mismo bloque de texto llano no resultará en el mismo bloque de texto cifrado, lo que dificulta el criptoanálisis. De hecho, ésta es la razón principal por la que se utiliza.

Modo de retroalimentación de cifrado

Sin embargo, el encadenamiento de bloques tiene la desventaja de que requiere la llegada de un bloque completo de 64 bits antes de que pueda comenzar la desencriptación. Este modo no es adecuado para terminales interactivas, en las que se pueden escribir líneas máximo de ocho caracteres y es necesario detenerse a esperar una respuesta. Para la encriptación byte por byte, modo de retroalimentación de cifrado, se utiliza (triple) DES. Para el AES la idea es exactamente la misma; sólo se utiliza un registro de desplazamiento de 128 bits.

Un problema con el modo de retroalimentación de cifrado es que si un bit del texto cifrado se invierte de manera accidental durante la transmisión, se dañarán los 8 bytes que se desencriptan mientras el byte incorrecto se encuentra en el registro de desplazamiento. Una vez que el byte incorrecto se elimine del registro de desplazamiento, se generará nuevamente texto llano correcto. Por lo tanto, los efectos de un solo bit invertido se limitan relativamente a un sitio y no se daña el resto del mensaje, pero sí se dañan los bits que haya en el registro de desplazamiento.

Modo de cifrado de flujo

Existen aplicaciones en las que un error de transmisión de 1 bit que arruina 64 bits de texto llano es demasiado. Para estas aplicaciones, existe una cuarta opción, el modo de cifrado de flujo. Funciona encriptando un vector de inicialización y usando una clave para obtener un bloque de salida. A continuación se encripta este bloque usando la clave para obtener un segundo bloque de salida. A continuación este bloque se encripta para obtener un tercer bloque, y así sucesivamente. La secuencia (arbitrariamente grande) de bloques de salida, llamada flujo de claves, se trata como un relleno de una sola vez y se le aplica OR exclusivo con el texto llano para obtener el texto cifrado. Es esencial nunca utilizar dos veces el mismo par con un cifrado de flujo, pues de hacerlo generará cada vez el mismo flujo de claves. Utilizar dos veces el mismo flujo de claves expone al texto cifrado a un ataque de reutilización de flujo de claves.

Modo de contador

Los archivos de disco con frecuencia se acceden en orden no secuencial, especialmente los archivos de bases de datos. Con un archivo encriptado mediante encadenamiento de bloques de cifrado, el acceso a un bloque aleatorio requiere que primero se desencripten todos los bloques que estén delante de él, lo cual es muy costoso. Por esta razón, se ha inventado otro modo, el modo de contador. Aquí el texto llano no se encripta en forma directa. En su lugar, se encripta el vector de inicialización más una constante, y al texto cifrado resultante se le aplica un OR exclusivo con el texto llano. Al incrementar en 1 el vector de inicialización por cada nuevo bloque, es más fácil desencriptar un bloque en cualquier parte del archivo sin tener que desencriptar primero todos sus predecesores.

Otros cifrados

DES y Rijndael son los algoritmos criptográficos de clave simétrica más conocidos. Sin embargo, vale la pena mencionar que se han diseñado otros cifrados de clave simétrica. Algunos de ellos están incluidos en varios productos.

Criptoanálisis

Cuatro avances recientes del criptoanálisis

El criptoanálisis diferencial:(Biham y Shamir, 1993). Esta técnica puede utilizarse para atacar cualquier cifrado en bloques; empieza con un par de bloques de texto llano que difieren sólo en una cantidad pequeña de bits y observando cuidadosamente lo que ocurre en cada iteración interna a medida que avanza la encriptación. En muchos casos, algunos patrones son mucho más comunes que otros, y esta observación conduce a un ataque probabilístico.

El criptoanálisis lineal: (Matsui, 1994). Éste puede descifrar el DES con sólo 243 textos llanos conocidos. Funciona aplicando un OR exclusivo a ciertos bits del texto llano y el texto cifrado en conjunto y buscando patrones en el resultado. Al hacerse repetidamente, la mitad de los bits deben ser 0s y la otra mitad 1s. Sin embargo, con frecuencia los cifrados introducen una desviación en una dirección o en la otra, y esta desviación, por pequeña que sea, puede explotarse para reducir el factor de trabajo.

El análisis del consumo de energía eléctrica: para averiguar las claves secretas. Si un algoritmo criptográfico consiste en un ciclo en el que los bits clave se procesan en orden, un atacante que reemplace el reloj principal de n GHz con uno lento (por ejemplo, 100 Hz) y coloque pinzas de caimán en los pines de energía y tierra de la CPU, puede monitorear con precisión la energía consumida por cada instrucción de la máquina. A partir de estos datos, deducir la clave es sorprendentemente fácil.

El análisis de temporización: Si las partes then y else toman diferentes cantidades de tiempo, reduciendo la velocidad del reloj y viendo el tiempo que tardan en ejecutarse varios pasos, también podría ser posible deducir las claves de ronda. Una vez que se conocen todas las claves de ronda, por lo general puede calcularse la clave original. Los análisis de energía y temporización también pueden utilizarse de manera simultánea para facilitar el trabajo.

ALGORITMOS DE CLAVE PÚBLICA

Históricamente el problema de distribución de claves siempre ha sido la parte débil de la mayoría de los criptosistemas. Sin importar lo robusto que sea un criptosistema, si un intruso puede robar la clave, el

sistema no vale nada. Los criptólogos siempre daban por hecho que las claves de encriptación y desencriptación eran la misma

En 1976, dos investigadores de la Universidad de Stanford, Diffie y Hellman (1976), propusieron una clase nueva de criptosistema, en el que las claves de encriptación y desencriptación eran diferentes y la clave de desencriptación no podía derivarse de la clave de encriptación, tenían que cumplir con los tres requisitos siguientes.

El primer requisito dice que, si aplicamos D a un mensaje cifrado, E(P), obtenemos nuevamente el mensaje de texto llano original, P. Sin esta propiedad, el receptor legítimo no podría desencriptar el texto cifrado. El segundo requisito no requiere explicación. El tercer requisito es necesario porque, como veremos en un momento, los intrusos pueden experimentar a placer con el algoritmo. En estas condiciones, no hay razón para que una clave de encriptación no pueda hacerse pública

El algoritmo RSA:

La única dificultad estriba en que necesitamos encontrar algoritmos que realmente satisfagan estos tres requisitos. Debido a las ventajas potenciales de la criptografía de clave pública, muchos investigadores están trabajando a todo vapor, y ya se han publicado algunos algoritmos. RSA. Ha sobrevivido a todos los intentos para romperlo por más de un cuarto de siglo y se le considera muy robusto. Mucha de la seguridad práctica se basa en él. Su mayor desventaja es que requiere claves de por lo menos 1024 bits para una buena seguridad.

La seguridad del método se basa en la dificultad para factorizar números grandes. Si el criptoanalista pudiera factorizar n (conocido públicamene), podría encontrar p y q y, a partir de éstos, z. Equipado con el conocimiento de z y de e, puede encontrar d usando el algoritmo e Euclides. Afortunadamente, los matemáticos han estado tratando de factorizar números grandes durante los últimos 300 años, y las pruebas acumuladas sugieren que se trata de un problema excesivamente difícil

Otros algoritmos de clave pública

Históricamente el problema de distribución de claves siempre ha sido la parte débil de la mayoría de los criptosistemas. Sin importar lo robusto que sea un criptosistema, si un intruso puede robar la clave, el sistema no vale nada. Los criptólogos siempre daban por hecho que las claves de encriptación y desencriptación eran la misma En 1976, dos investigadores de la Universidad de Stanford, Diffie y Hellman, propusieron una clase nueva de criptosistema, en el que las claves de encriptación y desencriptación eran diferentes y la clave de desencriptación no podía derivarse de la clave de encriptación, tenían que cumplir con los tres requisitos siguientes. El primer requisito dice que, si aplicamos D a un mensaje cifrado, E(P), obtenemos nuevamente el mensaje de texto llano original, P. Sin esta propiedad, el receptor legítimo no podría desencriptar el texto cifrado. El segundo requisito no requiere explicación. El tercer requisito es necesario porque, como veremos en un momento, los intrusos pueden experimentar a placer con el algoritmo. En estas condiciones, no hay razón para que una clave de encriptación no pueda hacerse pública.